**BUILDING DEMO PROJECT WITH WEB SERVICES FOR VERIFYING SIGNING EVALUATION FORM.**

This description page walks you through using web services to execute signing evaluation form verification algorithm.

**BACKGROUND.**

The evaluation form, which is signed by supervisor, will be sent to email server for verification. After many security actions, the form is finally encrypted then updated to trainee profile.

**WHAT TO BUILD.**

You will create 3 main features : data signing, data encryption and data verification.

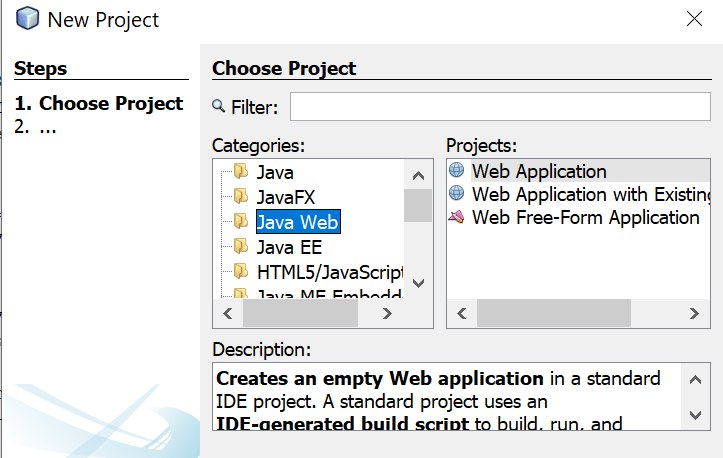
**TOOLS.**

* Netbeans IDE 8.2
* GlassFish Server 4.1.1
* Java EE 6 Web

**SET UP PROJECT WEB APPLICATION.**

In the New Project section, create a Java web application project.

Choose Java EE 6 Web and GlassFish Server 4.1.1 for initializing the project.



After successfully built the project, start a new Java Package. In this package, you need to create a Web Service. This Web Service is the server side where you will build scripts within.

**SECURITY STEPS**

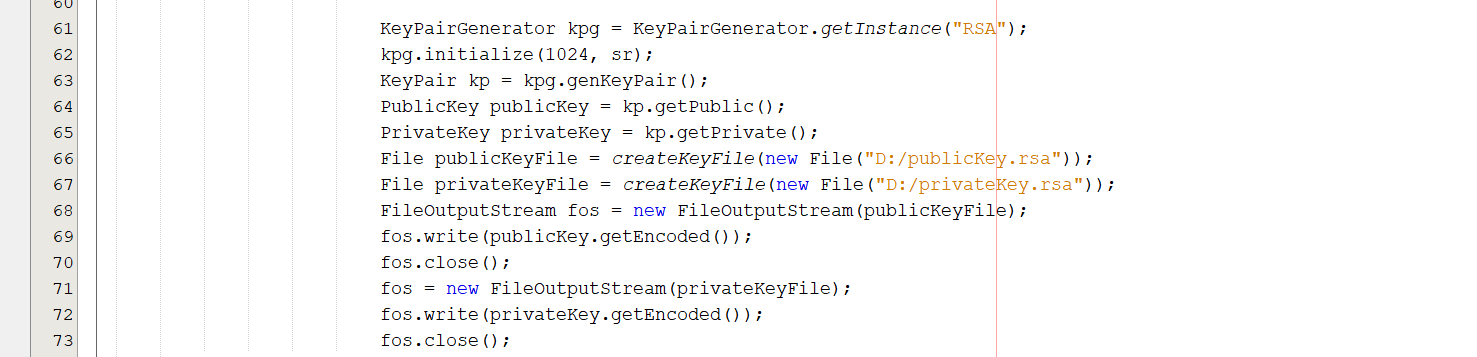
Signing data with supervisor private key then sending to email server.

Encrypting data with email server public key then sending to email server.

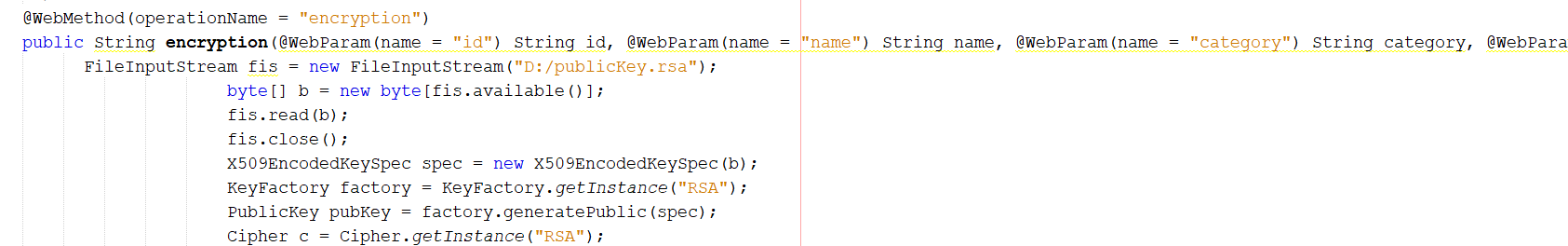
Email server will verify the signed and encrypted data by comparing their hash.

**BUILD JAVA FUNCTIONS**

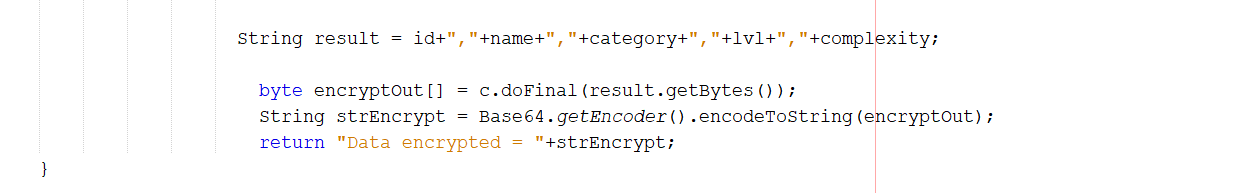
Starting simple, create a String value for inputting basic information in the evaluation form. This String value will go through RSA method for encryption and decryption.



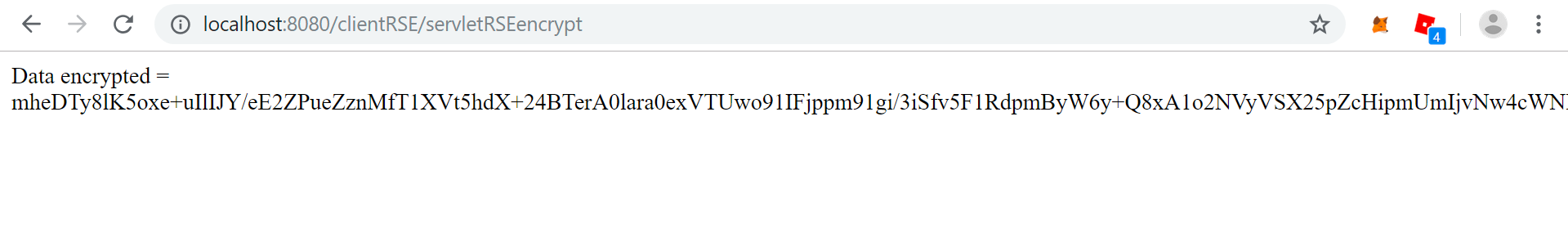
First, create a key pair for generating email server Public and Private Key.



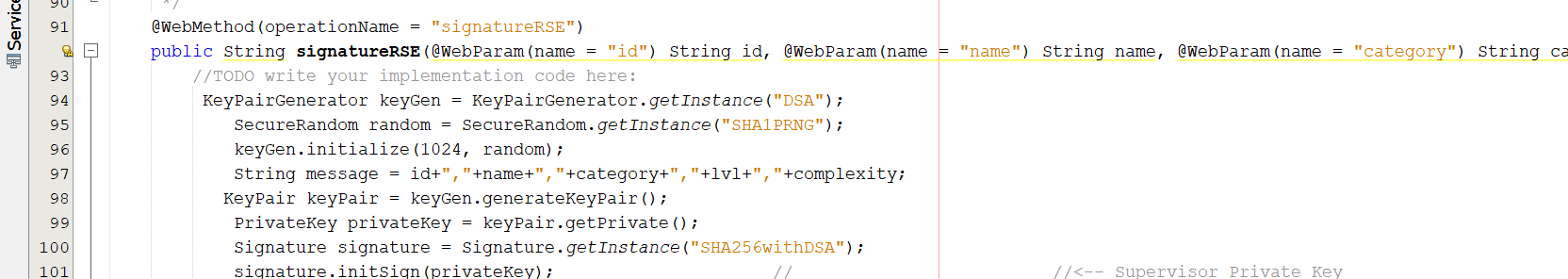
Basic information will be like ID, name, category, level of supervision and complexity.



Information will be stored in result value then encrypted using email server public key to be a random string of characters. And that’s all data encryption function.

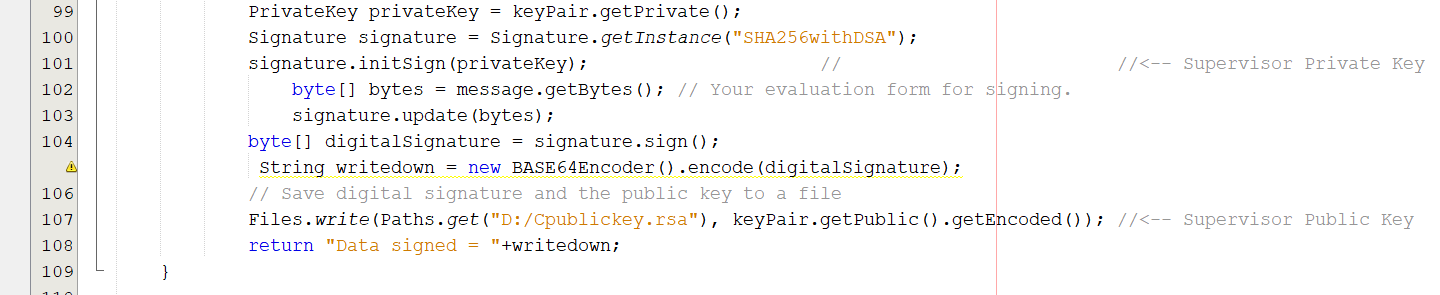


Unlike the encryption part, the String signature value will generate the key pair independently within the program. This key pair is owned by supervisor for signing the evaluation form.



The signature object is created along with the specified signature algorithm SHA256withDSA.

The object is then initialized for signing, with supervisor private key.

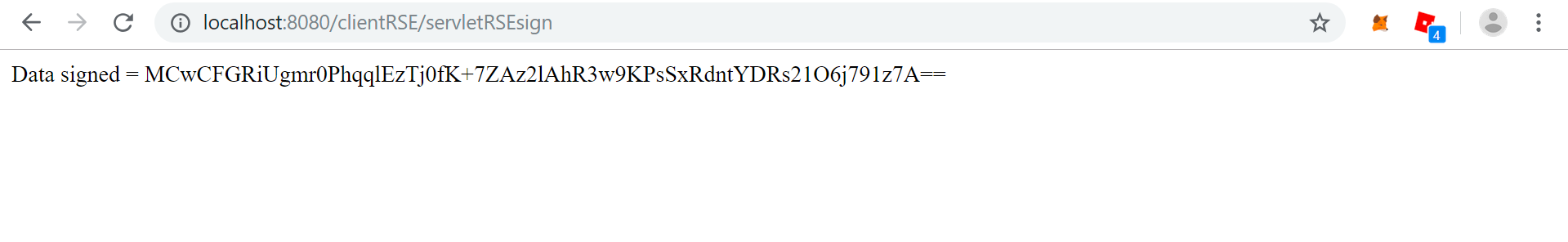


The String message, which contained basic information for evaluation form, will be updated to the signature object to be signed by supervisor private key.

After is updated, it will return the signature in bytes form to byte[] digitalSignature.

String writedown is used for printing the data signed to supervisor screen.

Also, the newly created supervisor Public Key will be written to a file then moved to the verification algorithm for verifying.



Copy this signature and move to the next step : Verification algorithm.

In the verifying program, you only need to enter 2 values : data signed and data encrypted.

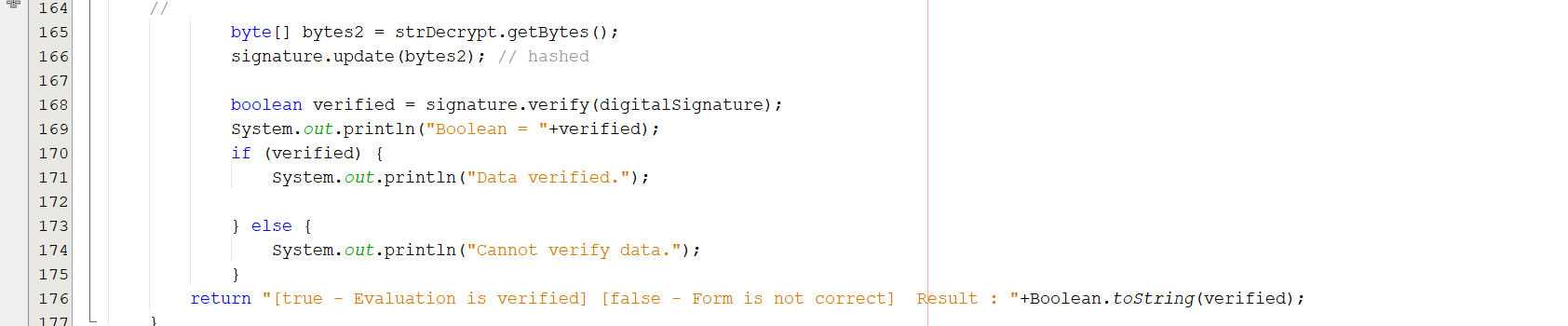
The data signed will be converted to bytes form for hashing.



Supervisor public key will be assigned to the newly created signature : to initialize the object for verifying. With the same signature algorithm SHA256withDSA.

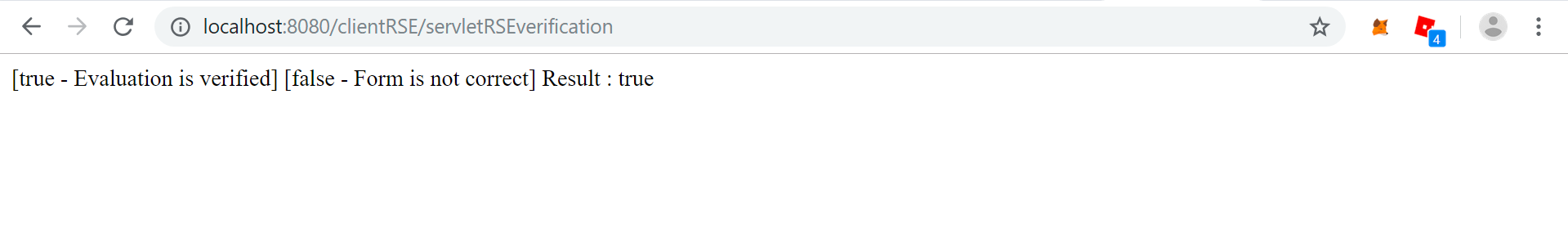


Now we will use email server private key to decrypt the data. Data is now in it original form, after is safely sent to email server.



The data will be updated in the signature object for hashing.

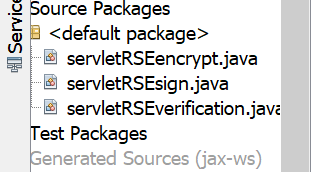
The verify() method will hash and compare the hashed data (signature) and hashed signature (digitalSignature)



In the final result, it printed Result : true, which mean the data is correct. If not, the result will return a false value.

**BUILD JAVA SERVLET**

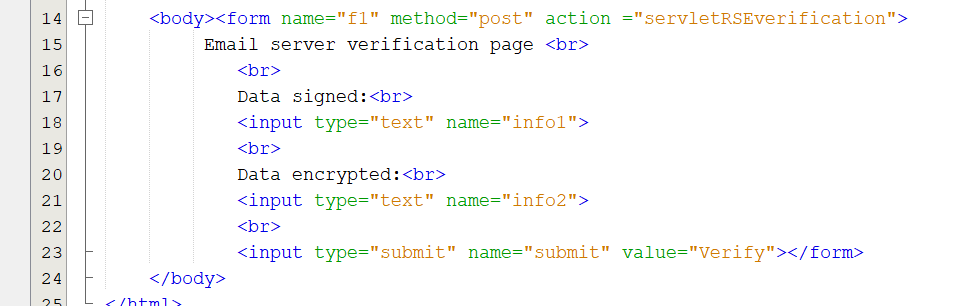
In order to run these Java functions, you need to build a servlet which will collect data inputs from end user through web page or specified database.



You need to build 3 different servlets which will output the executed data inputs from end user.

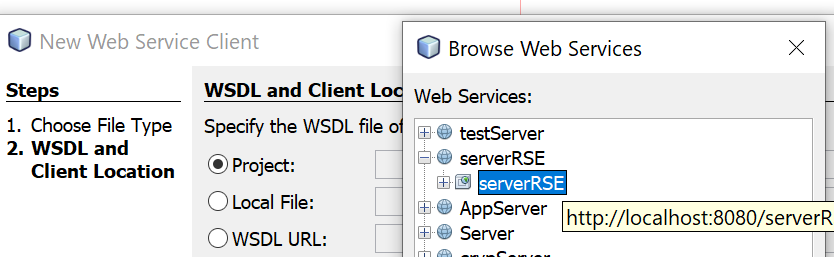






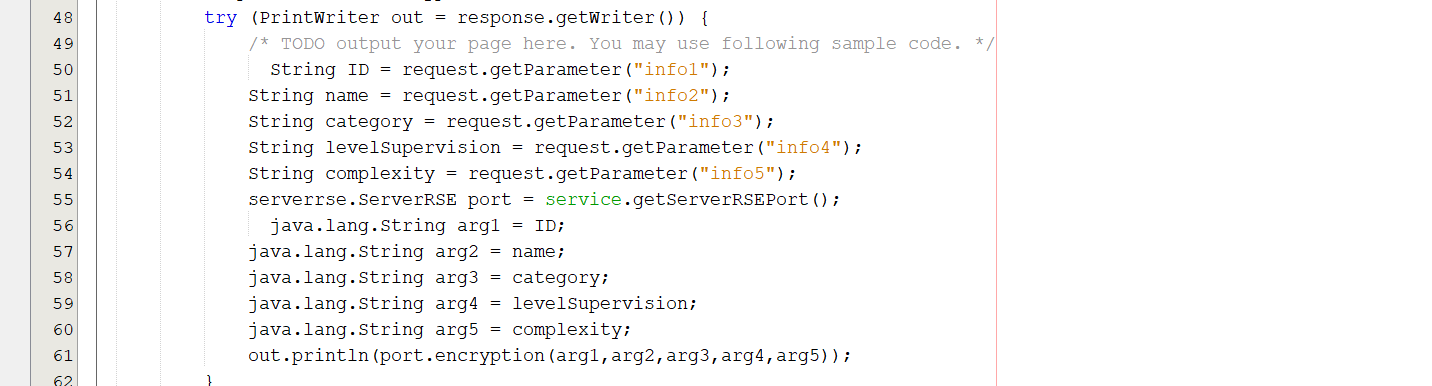
For each servlet, you’ll add text box and executing button for each functions in its JavaServer Page. So if you click the button, they will connect then return results from specified servlet.

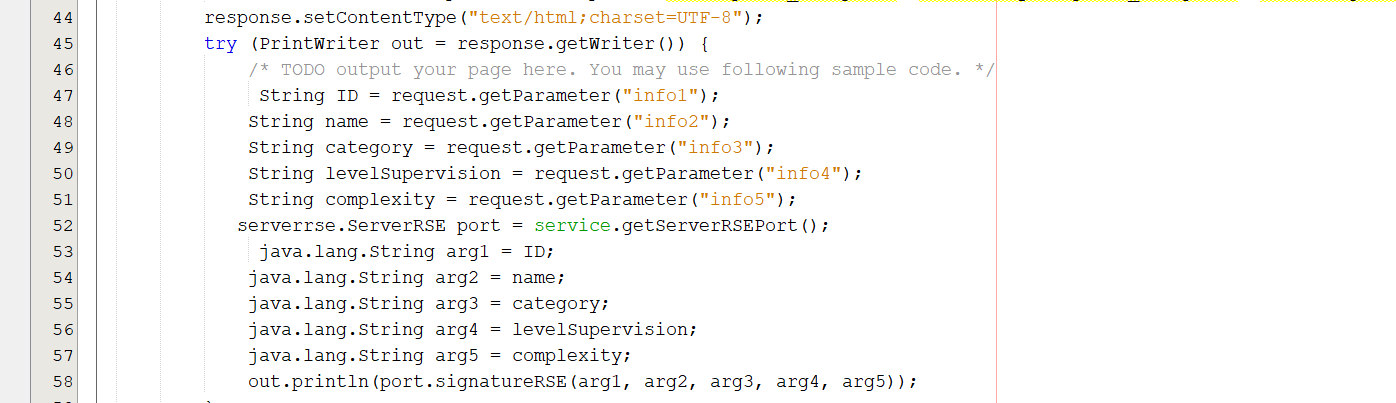
Note that the action attribute will specify where to send the data.

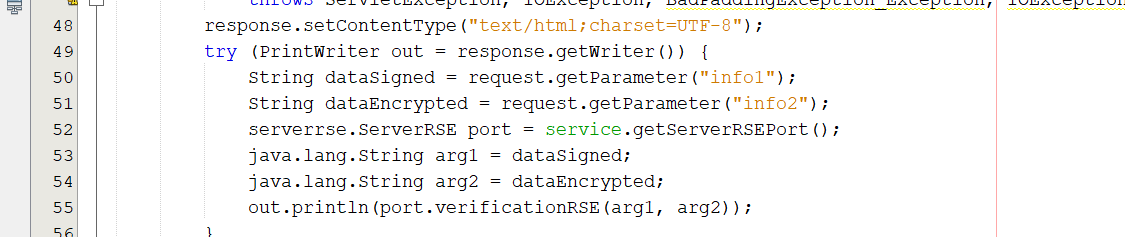


You will need to add a Web Service Client at your client servlet program. This Web Service Client will direct at your server program which runs the Java functions.

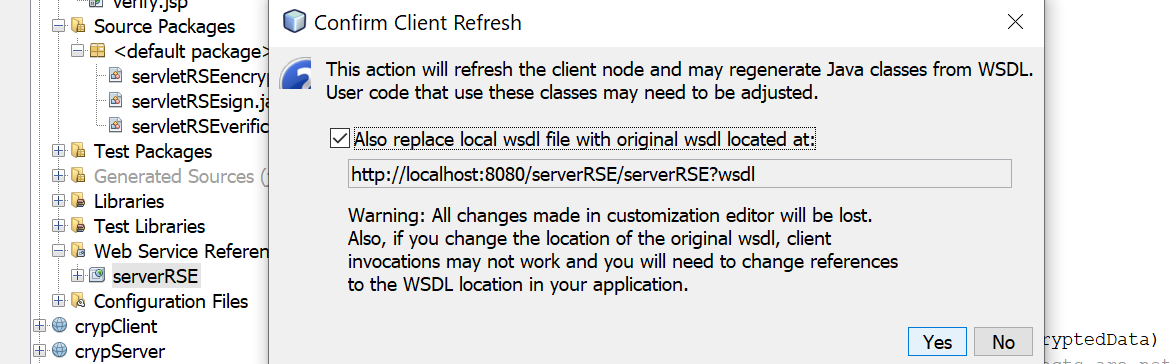
Each value will be requested by a specified parameter.





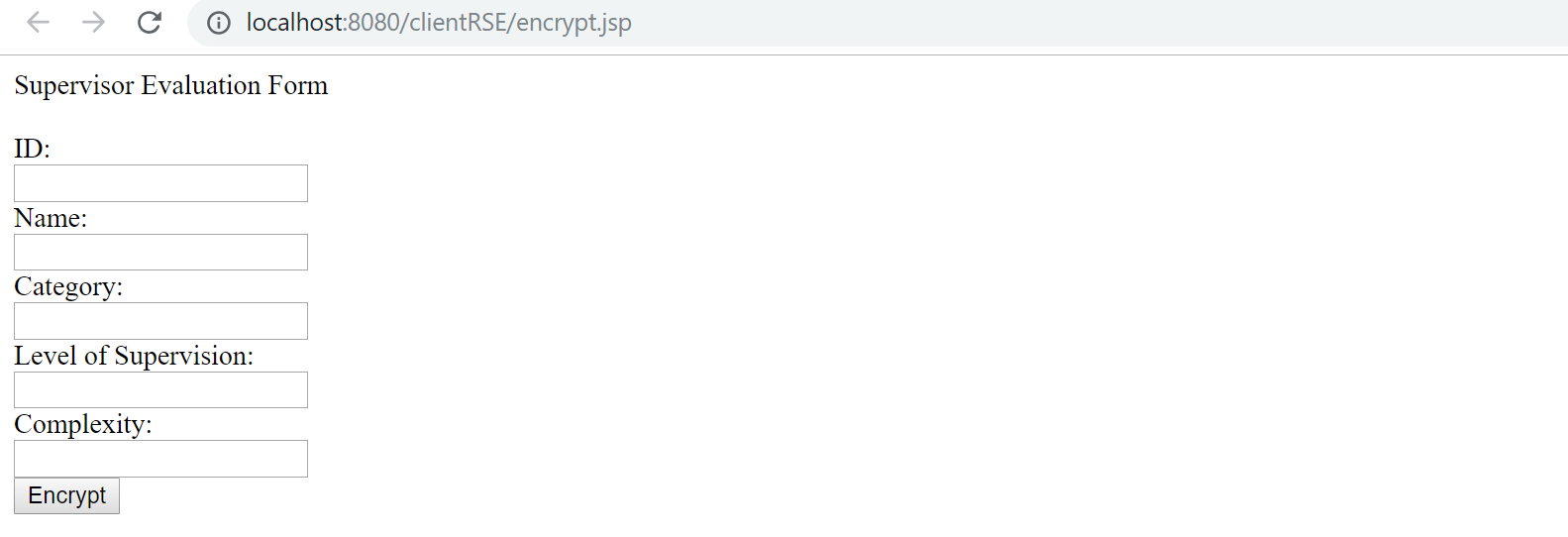


In the servlet, add port in the void main so it will print the value result to client page.

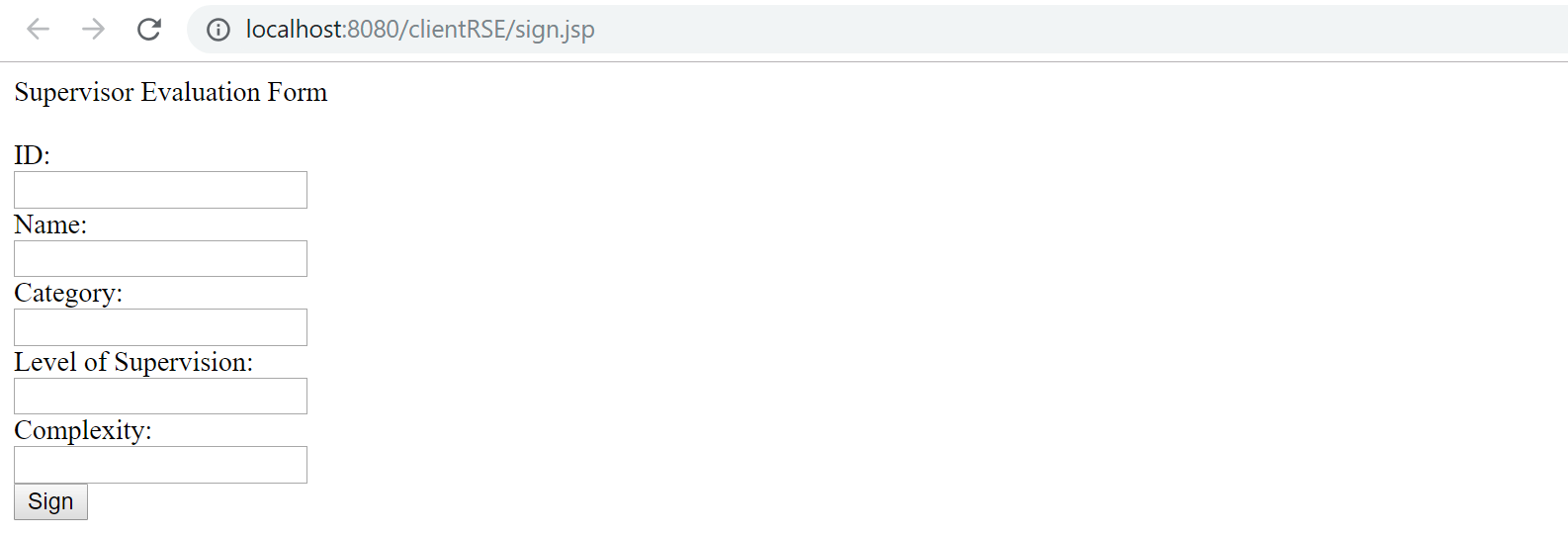


You will need to initialize your connection at address localhost 8080.

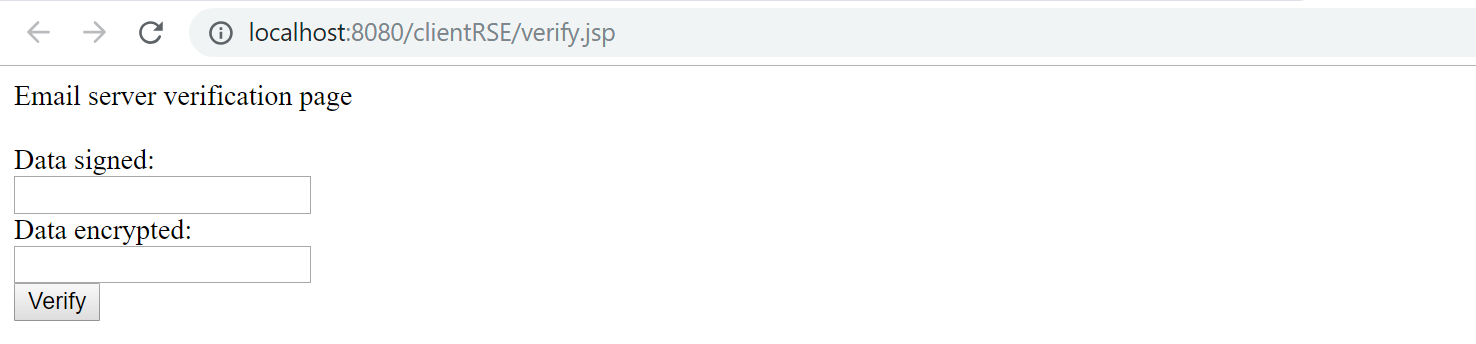
**END USER INPUT**



(Encrypting evaluation form by using email server public key)



(Signing evaluation form by using supervisor private key)



(Input signed data and encrypted data for verifying the evaluation form)